County of Santa Clara
Office of the District Attorney Surveillance Use Policy

Video Surveillance and Recording of Evidence Storage Facility

1. Purpose

The Santa Clara County District Attorney's Office (SCCDA) maintains an off-site and secure evidence storage facility that is not open to the public. The facility shall be used for storage of evidence items collected during criminal investigations, such as contraband, narcotics, and firearms. The facility is equipped with a network video recorder (NVR) surveillance system that records activity within the storage facility to maintain the integrity of the evidence.

The facility is currently equipped with cameras manufactured by Axis Communications and Arecont Visions, with technologies such as day/night support, low-light support, high definition video, optical zoom, and pan/tilt/zoom (PTZ). The NVR system shall permit remote monitoring using a web browser or mobile application, which gives authorized users the ability to monitor live video feeds and perform basic playback functions while offsite. The system is integrated into the intrusion-detection system and sends authorized users video clips as alerts when unauthorized movement is detected. Lastly, the system has the capacity to record video-only when motion is detected to efficiently utilize a finite video repository.

2. Authorized and Prohibited Uses

Use of the NVR system in the evidence storage facility shall be limited to only SCCDA personnel authorized by SCCDA Administration to use the system in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA. Any monitoring of the system or exporting of stored data shall be done pursuant to this Surveillance Use Policy and applicable state and federal law. To limit any expectation of privacy, signage shall be posted on-site to indicate the presence of video monitoring.

County-owned video surveillance and associated recordings shall not be used for personal, non-SCCDA purposes. The video surveillance equipment shall not be used for illegal purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

3. Data Collection

The NVR system shall only record activity within the SCCDA's off-site evidence storage facility and transmit that encrypted data in real time to a SCCDA computer server stored on site. The recorded data shall be automatically stored in the server within the finite storage capacity for the system, unless authorized SCCDA personnel export data for a specific authorized, case-related or administrative purpose.

//

4. Data Access

The NVR surveillance system shall be stored in a secure location and access to the system shall be documented in an activity log. The data collected by the NVR surveillance system shall be stored in the physical case file and/or stored within an SCCDA-approved electronic case/content management system. Approved case/content management systems shall log user name, date/timestamp, files or data accessed, and attempts at altering or deleting files.

Access to the NVR system and exported data shall be limited to SCCDA personnel authorized by SCCDA Administration to utilize the system and exported data in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA, as well as other county personnel designated in writing by the District Attorney or the District Attorney's written designee to the extent they believe that access is reasonably necessary for a specific criminal, civil, or administrative investigation or action.

5. Data Protection

See Sections 3 and 4 of this Policy. The County of Santa Clara and the SCCDA shall utilize physical access controls, application permission controls, and other technological, administrative, procedural, operational, and personnel security measures to protect the data collected by the NVR surveillance system from unauthorized access, destruction, use, modification, or disclosure. The NVR system shall be housed in a secured law enforcement facility with multiple layers of physical security and security protection. All data exported from the NVR system shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

6. Data Retention

NVR system data, whether downloaded, copied or printed, shall be maintained in accordance with this Surveillance Use Policy, applicable state and federal evidentiary laws, and the SCCDA Record Retention and Destruction Policy approved by the Board of Supervisors on June 21, 2016, as follows:

Case Type	Official Retention Period
Homicide Case Files	Permanent
All Non-Homicide Case Files, Unless Otherwise Stated in this Schedule	Seventy-five years. Case files will be scanned and electronically archived and retained for 75 years. Originals will be retained for a period of at least 90 days to allow scanning for authentication by the department, after which they will be destroyed. Backed up by DA IT provider.

Case Type	Official Retention Period
Juvenile Ward Files	When a minor turns 18 and petitions the court for records to be sealed, the record will be destroyed at age 20 or as otherwise ordered by a court of competent jurisdiction. Otherwise as covered by this schedule.
Developmentally Disabled (DD) Case Files	Life of the defendant.
Plea of Insanity (PC 1026) Case Files	Life of the defendant.
Juvenile Case Files	Two years after final disposition or until minor attains age of 21, whichever is later. Caveat 1): If case is appealed, the file must be retained until the final appellate decision is received. Caveat 2): Cases that may be charged as "strikes" should be retained for 75 years.
Certificates of Rehabilitation Case Files	Two years.
Advise and Assist Case Files	Two years.
Expungement Case Files	Two years.
Post-Conviction Proceedings and Special Project Files	Two years.

Data that is relevant to administrative/personnel-related matters shall be downloaded or otherwise copied, and retained through the adjudication of any administrative, civil or criminal case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations. To the extent that data is not covered in the chart above, the data shall be destroyed no later than two years after the later of (1) the time for an appeals process expires; (2) the statute of limitations expires; and (3) for data regarding a County employee's administrative investigation, the date the employee's employment for the County terminates. All data stored in the system shall be purged no later than one year from the date it was collected.

7. Public Access

Absent a court order, the public shall not have direct access to data collected by the video surveillance and recording system in the evidence storage facility. If a California Public Records

Act request, subpoena, or court order is issued for this data, it shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Office of the County Counsel as needed.

8. Third-Party Data-Sharing

The sharing of data recovered through the NVR system shall be limited to the following third parties:

- Law enforcement agencies when relevant to an ongoing specific investigation or prosecution;
- Defense and appellate counsel and pro se litigants pursuant to Penal Code section 1054 et seq. and *Brady v. Maryland*;
- Individuals who have obtained a valid Court Order, subpoena, or otherwise approved in writing by the District Attorney or written designee.

9. Training

SCCDA shall provide staff with a copy of this Surveillance Use Policy when training on the secure handling of confidential and personal information, including data collected by the video surveillance system in the evidence storage facility. The training shall address appropriate handling and transmission procedures, as well as consequences of misuse of the data and a security breach.

10. Oversight

District Attorney's Office Administration shall ensure compliance with this Surveillance Use Policy and all applicable laws. The NVR system shall employ an audit feature that tracks access and activity, user name, date/timestamp, files or data accessed, and attempts at altering or deleting files. SCCDA Administration shall conduct audits of the system as it deems necessary, and at least annually, to ensure appropriate use of the system. Sanctions for violation of this Surveillance Use Policy or applicable laws may range from counselling to termination, and in more serious breaches, may result in criminal prosecution.

Approved as to Form and Legality

Rob Coelho 10/29/18

Rob Coelho
Office of the County Counsel